АНОТАЦІЯ

Криптоаналіз потокових шифрів в високопродуктивних обчислювальних системах // Дипломна робота // Вітрук Ігор Вікторович // Тернопільський національний технічний університет імені Івана Пулюя, Факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних систем та мереж, група СІм-61 // Тернопіль, 2014 // с. – 175, рис. – 17, табл. – 21, кресл. – 9, бібліогр. – 7.

Ключові слова: ANF, A5/1, CNF, Cryptominisat, DIMACS, DPLL, Grain of Salt, GSM, LFSR, SAT, NP-повна задача, криптоаналіз, алгебраїчний криптоаналіз, криптостійкість, булеві функції, потокові шифри, лінеаризація, високопродуктивні обчислення, декомпозиція, XL-алгоритм, обчислювальні кластери.

Робота присвячена оптимізації криптоаналізу потокових шифрів шляхом використання вдосконаленого методу перетворення систем рівнянь з АНФ у КНФ, а також використання методів паралельно-розподіленого розв'язання задач, зокрема методу крупноблокового розпаралелення (декомпозиції за даними). Зважаючи на широку сферу застосування потокових шифрів, існуючі сучасні методи їх криптоаналізу, запропоновано методи для ефективного дослідження криптостійкості відомих потокових шифрів. Проаналізовано сучасні методи криптоаналізу та обрано найбільш оптимальний та ефективний метод – алгебраїчний криптоаналіз. Обґрунтовано математичний апарат для перетворення з АНФ до КНФ та запропоновано методи оптимізації таких перетворень. Розроблено інформаційну систему для здійснення алгебраїчного криптоаналізу в високопродуктивних обчислювальних системах на базі технологій та мов: OpenMosix, Java, Prolog, Sat4J та, альтернативно, Cryptominisat та Grain of Salt. Використовуючи розроблену систему проведено криптоаналіз потокового шифру A5/1. Керуючись проведеними дослідженнями сформульовано рекомендації по підвищенню криптостійкості потокових шифрів та їх застосуванню.